Building Self-Adaptive Cyber Physical Systems Using Unreliable Components

Weisong Shi and Shinan Wang
Wayne State University
{weisong,shinan}@wayne.edu

1. Introduction

Modern automobiles, featuring increased convenience, safety, and energy savings, have become more and more reliant on the outcomes of the IT industry. Existing services such as vehicle tracking, navigation and emergency notification envision a promising future of more powerful computing-assisted automobile systems. Some examples include remote vehicle controllers, short range braking systems, and eventually, the self-guided automobile could drive instead of human beings. However, with established techniques, designers could barely implement more advanced systems due to several specific requirements of future CPS. First, the system has to be very reliable. However, the sensing data are not reliable given the harsh physical world where sensors are deployed and operated. Second, adaptation is the key to the success of CPS, but to the best of our knowledge, we haven't seen a mature theoretical model that can guide the adaption. Finally, as technologies have gradually immersed into our personal lives, how much should we trust and rely on the *technology*, and who will be responsible for the mistakes?

2. Three Challenges

Unreliable Input vs. Reliable Systems Existing networking systems have suffered from malicious and nonsensical data while being attacked. The case could be worse in mission-critical systems, such as automobiles, rail, and aviation systems because data collection devices like sensors work in a more hash and open environment than those of traditional networking systems, making inaccurate, redundant data as well as attacks a common phenomenon, rather than exceptional. Additionally, the most fundamental difference between CPS and traditional systems is that time plays an essential role in CPS. The real physical world presents a large seamless concurrent unit, bringing more uncertainties to systems than a real-time system can handle. More specifically, sensors are typically designed to detect one particular parameter, like the speed of automobiles on a highway, the density of a busy freeway, or whether a speeding vehicle is an ambulance or a police car. Reported events like that will bring our systems a large amount of unnecessary data. Obviously, unreliable data would be inevitable and an impediment to the progress of CPS design. However, to extract true information from unreliable data, while providing reliable services is not impossible. [1] lists the whole spectrum of data management in sensor networks, suggesting two relating subfields in manipulating sensor data: statistical modeling, data uncertainty handling. For the former approach, some researchers suggested to insert statistical models into a database system like [2] and [3]. Regarding data uncertainty, many approaches refer probability theory as a basis, with much of the related research focusing on building a probabilistic database. Also, attaching trust, reputation or accuracy to the database becomes a common topic, like how [4] described a data management approach with respect to data consistency. While concentrating on dealing with unreliability, none of the existing research could handle all possible situations well. Hence, a great deal of specific research is needed in this realm.

Adaptation vs. Agility Robustness and efficiency used to be two key issues in system design. When faced with a much more complex reality, we argue that these two requirements are insufficient. In fact, only an agile system could fit the urgent needs of CPS. From a system design point of view, one of the essential motivations of a CPS target is to make the current transportation system more efficient and less energy consuming, requiring flexible control over automobiles as well as traffic management systems. Consider the following scenario, when a driver faces an intersection during non-rush hour, and no vehicles are crossing the intersection, but a red signal stops the driver. This is both annoying and a waste of resources to the traffic system. More typically, road blocking often increases the workload of other parallel highways or freeways, so the question is how to reduce the possibility of traffic jams on other roads in such cases? Future CPS is capable of handling such situations well by temporarily adjusting traffic rules to optimize the situation. An example is the allowance for automobiles in the aforementioned case to keep moving. However, with the flexible and frequent changing of current restrictions on traffic control, another issue arises, how agile do systems need to be? Particularly, when dealing with life-threatening issues, the bottom line is to prevent system disorder and chaos. What is the range between making systems more agile and allowing them to be too loose to control? In addition, another trade-off issue arises. Future CPS should featured as environment-aware, which differentiates from existing complication trade-offs because of the infinite complexity of the physical world compared to finite algorithms and system resources. Besides, a well-known characteristic of the physical world, but often ignored currently leads systems to be fragile and vulnerable. For instance, it is relatively doable to optimize part of CPS, which might trigger potential chaos to the system as a whole, like the butterfly effect-- when every corner of the system adjusts its rules, how does it react to the whole picture?

Whose Responsibility: Human vs. CPS? CPS design becomes more and more challenging than traditional computer system design in that CPS places accountability at a much higher level than traditional systems, because it is a miss-critical and life-threatening system. Issues abound, such as how do customers interact with CPS? Are they partially integrated in the existing normal system or do they fully depend on the advanced conveniences offered by CPS? For example, when an emergency happens on a freeway, would systems release the control of automobiles to drivers or not? If not, would drivers allow their lives to be in the sole control of machines? Nowadays, pilots depend on sophisticated embedded systems for navigation when flight paths are comparatively stable, while more dangerous operations like taking off and landing still count on experience and personal judgment. In the future, system designers should decide whether it is necessary to let pilots make such critical decisions based on the suggestion of systems or completely trust operations taken by systems. The chain consequences might involve tremendous social impacts. For example, if an accident happens, who is responsible for that? Is it the driver or pilot who makes his/her own improper manipulation or the systems' incompleteness and calculating errors that lead to crash? Furthermore, due to the potential social impact of CPS, we envision the necessity for an interdisciplinary investigation, allowing research about the human-machine relations before advanced CPS systems can be put into practice.

3. Three Requirements/Innovations of CPS Systems

Needs trigger innovations. It is apparent that traditional networks, control mechanisms and operating systems barely satisfy the demands of modern CPS in that they emphasize less on both the adaptive features and the notion concurrent. Specifically, we envision the following three required areas that deserve innovations.

Novel programming language/environment The physical world presents both spatially and temporally. Hence, what is the best way to program in the context of CPS? We might need a new programming language that allows us to integrate the spatiotemporal information easily into the program. Novel programming tools would be considered as a bridge component or an interface, which connects the low-level data points to the upper level of applications. However, this is not the whole story, as the agility requirement aforementioned; the new programming language will have to provide an efficient mechanism to deal with feedback control, which is a core abstraction in cyber-physical systems. In summary, programming the physical world is different from traditional declarative or imperative programming languages, and thus we might need to introduce a brand new programming paradigm for CPS.

Environment-aware middleware. Although wireless sensor networks provide relatively timely information in regards to the surroundings, too heavy of a work load is left to the upper layers, which probably includes, but is not limited to, identifying the objects of parameter, rearranging the sequence of events, filtering redundant and deceptive data, weighting parameters, and making decisions. Environment-aware middleware could provide what future CPS needs but the current system asks too much of the upper layers. For example, it requires the collection of an "information set" rather than single data set. Information sets could integrate raw data from the sensors to form more meaningful information to be handled more easily by the upper layer, including information such as temperature, moisture and traffic density associated with a particular time point.

Verification and evaluation tools. Apparently, the unpredictable physical world impedes the development of system design verification, and evaluation procedures. The method needed to verify the feasibility and efficiency of newborn systems would not be easier than designing the system itself. The wide acceptance of CPS will definitely rely on the available of these tools. The tools for CPS will have to consider several unique metrics, such as the fatalness of the systems since most of these systems are life threatening. This is distinctly different from many of the tools for traditional computer systems research,

References

[1] M. Balazinska et al. Data management in worldwide sensor web, IEEE Pervasive Computing, June 2007.

[2] A. Deshpande and S. Madden, “MauveDB: Supporting Model-Based User Views in Database Systems,” Proc. 2006 ACM SIGMOD Int’l Conf. Management of Data, ACM Press, 2006, pp. 73–84.

[3] M.J. Egenhofer, “Toward the Semantic Geospatial Web,” Proc. 10th ACM Int’l Symp. Advances in Geographic Information Systems (GIS 02), ACM Press, 2002, pp. 1–4.

[4] Kewei Sha and Weisong Shi, “Consistency-Driven Data Quality Management in Wireless Sensor Networks,” accepted by Journal of Parallel and Distributed Computing June 2008.